UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/534,855	05/13/2005	Michel Mahieu	28944/40154	9106

29471 7590 03/09/2010
MCCRACKEN & FRANK LLP
311 S. WACKER DRIVE
SUITE 2500
CHICAGO, IL 60606

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
03/09/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/534,855	**Applicant(s)** MAHIEU, MICHEL	
	Examiner MICHAEL R. VAUGHAN	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 January 2010*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *45-54 and 56-85* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *45-69,71-78 and 83-85* is/are rejected.

7)☒ Claim(s) *70, 79-82* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on **1/21/10** has been entered.

Claims 45-54 and 56-85 are pending. Claim 55 has been cancelled.

Response to Amendment

Claim Objections

Claims 45, 48, 53, 54, 72, and 83 are objected for the following informalities:

As per claims 45 and 83, the term "a component" is used in the simulation phase after a start component and a finish component have been defined. It is unclear which component of the set of components is changing state.

As per claim 48, the term and/or is indefinite because of its dual meaning.

Regarding claims 53, 54, and 72, the phrase "for example" renders the claim indefinite because it is unclear whether the limitation(s) following the phrase are part of the claimed invention.

Response to Arguments

Applicant's arguments with respect to claims 45-54 and 56-85 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 45-54, 55-57, 58-69, 71-78, and 83-85 are rejected under 35 U.S.C. 103(a) as being unpatentable over NPL “Network Security Modeling and Cyber Attack Simulation Methodology” to Sung et al. published 7/11/01, hereinafter **Sung** in view of USP 6,952,779 to Cohen et al., hereinafter **Cohen** and USP 6,535,227 to Fox et al., hereinafter **Fox**.

With respect to claim 45, Sung teaches the limitation of a “modeling phase, comprising creation of a virtual system [modeled network in S/W environment; pg. 322] comprising a specification of an architecture of the information system with a graphical representation of a set of components of the information system and relations between said set of components, each component being associated with at least one state initialized with a sound value, the relations between two determined components comprising propagation relations able to convey attacks, and a specification of first and second sets of behavioral rules, the first set of behavioral rules from the standpoint of the operation of the system [framework and underlying modeled network functionality] and the second set of behavioral rules from the standpoint of security [how the nodes respond to attacks], associated with the components of the system, each behavioral rule comprising one or more predicates and/or one or more actions" (page 321, lines 10-18) as the network security modeling and cyber attack simulation employing the advanced modeling and simulation concepts that supports a hierarchical and modular modeling environment, which (page 323, lines 7-14) consists of a system entity structure (SES) and model base (MB). The SES represents the knowledge of decompositions, taxonomies, coupling specification and constraints. The model base contains models that are procedural in character, expressed in discrete event system specification formalism. Furthermore (page 325, lines 18-20) dynamics of the component models can be represented in various ways according to their respective state variables. Sung teaches iteratively simulating potential attacks against the information system (pg. 327, lines 10-15). Finally, Sung discloses the graphical representation (Fig. 8; page 331, lines 1-8) as SECUSIM system where users can set up initial conditions for simulation by using windows of each node. Sung teaches implementing the modeling phase and the simulation phase on a computer that includes a man/machine interface and an attacks/parries engine (Fig. 8, page 331).

Sung does not explicitly disclose the construction of a local routing table making it possible to direct an attack through an attack path from a start component to a finish component. Cohen discloses the construction of a local routing table making it possible to direct an attack through an attack path from a start component to a finish component (col. 6, lines 47-55 and col. 7, lines 1-5). Both Sung and Cohen teach the simulation of attacks and generating topographical views of the network. Sung teaches the networks components are modeled including routers (Fig 7). Cohen teaches that routers are modeled to generate the network paths (col. 6, lines 55-60). Thus Cohen is able to plan an attack using a starting point and a target point in the network. This method could have easily been performed in the network attack simulation of Sung. The claim is obvious because one of ordinary skill in the art can combine known methods which produce predictable results.

Sung does not explicitly disclose the limitations that “each initialized state corresponds to a security status of each component in the context of attacks launched against the information system" and "updating the state of a component of the information system altered by a successful attack, wherein a successful attack causing a state of a component to pass to an unsound value”. These limitations are taught by Fox (col. 3, lines 40-58 and col. 9, lines 15-24). In Fox’s system a graphical representation of the network is shown. As attacks are simulated against the network the graphical representation of each network component are color coded. If an attack is successful against a component, its color changes to yellow or red depending on the severity of the attack. One of ordinary skill in the art could have combined this teaching with Sung to provide real-time feedback of network components to the user running the simulation. The claim is obvious because one of ordinary skill can combined known methods which produce predictable results.

With respect to claim 46, Sung teaches the limitation of “a name [service type] being associated with each component one or more adjectives [execution of each phrase] may also be associated with said component, which adjectives make it possible to designate said component without naming it” (pg. 326, Fig 5).

With respect to claim 47, Sung teaches the limitation of “determined states are associated with each component of the information system, each state being able to take a sound value [phases] and one or more unsound values” (pg. 326, Fig 5) as the server allows client to view the state of nodes and resources and (pg 331).

With respect to claim 48, Sung teaches the limitation of “certain at least of said states pertain respectively to the activity, the confidentiality, the integrity and/or the availability of the component with which they are associated” (pg 326, Fig. 5).

With respect to claim 49, Sung teaches the limitation of "an alleged name may be associated with any determined component, in particular in the case where said determined component is a usurper" as the name of the attackers are generate for each node (table 2).

With respect to claim 50, Sung does not teach the limitation of "a link to another component may be associated with any determined component, in particular in the case where said determined component is usurped and where said other component is a usurper". Cohen teaches that through the calculation of an attack path, adjacent nodes, dependent nodes, and nodes along the path may be identified and monitored (col. 6, lines 62-67). Examiner supplies the same rationale for the combination of Cohen and Sung as recited in the rejection of claim 45.

As per claim 51, Sung is silent in disclosing the propagation relations are bidirectional relations able to convey attacks in both directions. Cohen teaches this limitation as the system creates scenarios from the topology model to show potential attack paths (col. 6, lines 7-10). Examiner supplies the same rationale for the combination of Cohen and Sung as recited in the rejection of claim 45.

With respect to claim 52, Sung teaches the limitation of "the relations between any two determined components comprise service relations making it possible to designate a component on the basis of another component" (page 325, lines 17-20) as network component model comprises various services such as Telnet, Email, Ftp, Web, and Packet Filtering. The dynamics of these component models can be represented in various ways according to their respective stated variables.

With respect to claim 53, Sung teaches the limitation of “the behavioral rules comprise rules for propagating attacks, these rules being for example implemented in components which are vectors of attacks, and rules for absorbing attacks, these rules being for example implemented in components which are the target of attacks” (page 327, lines 10-12) as the attacker model outputs a sequence of attacking commands according to its attacking scenarios.

As per claim 54, Sung teaches the limitation of the behavioral rules comprise binary rules because the rules as followed by the simulation engine are interpreted by a computer, and thus their binary equivalent.

As per claim 56, Sung does not teach the local routing table is generated automatically according to the principle of the shortest path between the start component and the finish component. Cohen teaches this above limitation (col. 2, lines 10-15). Examiner supplies the same rationale for the combination of Cohen and Sung as recited in the rejection of claim 45.

With respect to claim 57, Sung fails to teach the attacks simulation step comprises the updating of the state of a component of the system altered by a successful attack. Fox teaches the limitation of “the attacks simulation step comprises the updating of the state of a component of the system altered by a successful attack” (col. 3, lines 40-58). Examiner supplies the same rationale for the combination of Fox and Sung as recited in the rejection of claim 45.

With respect to claims 59 and 60, Sung teaches the limitations of “the attacks comprise elementary attacks corresponding to unsound state values” (SYN flooding; pg 329, second paragraph) and “the attacks further comprise a special usurping attack (acquiring new access without a valid user ID; pg. 330)”.

With respect to claim 61, Sung teaches the limitation of “an attack is defined, in particular, by a type of attack, a type of protocol, and attack path elements” (table 2).

With respect to claim 62, Sung does not explicitly teach the limitation of “the attack path elements comprise a start component, a finish component, a target component, and as appropriate one or more intermediate components.”

On the other hand, Cohen teaches the abovementioned limitation (column 7, lines 1-2) as the system simulates attacks through the network topology from each start point to each end point. Examiner supplies the same rationale for the combination of Cohen and Sung as recited in the rejection of claim 45.

With respect to claim 63-66, Sung fails to teach the limitations of " the list of components already traversed by an attack is saved in one or more upstream stacks", “the upstream stacks comprise a stack containing the exhaustive list of all the components traversed, designated by their real name”, “wherein the upstream stacks comprise a stack containing the list of only those components traversed which are opaque, designated by their real name or, as appropriate, by their alleged name”, and “the list of destination components of an attack is saved in at least one downstream stack”. Cohen teaches the limitations of " the list of components already traversed by an attack is saved in one or more upstream stacks", “the upstream stacks comprise a stack containing the exhaustive list of all the components traversed, designated by their real name”, “wherein the upstream stacks comprise a stack containing the list of only those components traversed which are opaque, designated by their real name or, as appropriate, by their alleged name”, and “the list of destination components of an attack is saved in at least one downstream stack” (column 7, lines 25-35) as the attack simulation commences from a specified attack starting point. The system then loops through a moving front-line algorithm by repeatedly evaluating the constraints for every state/graph node that has not yet been reached. The moving front-line algorithm continues adding edges to new graph nodes until no more states/graph nodes can be reached at which point the process terminates. Examiner supplies the same rationale for the combination of Cohen and Sung as recited in the rejection of claim 45.

With respect to claim 67, Sung teaches the limitation of “the attacks are defined in a language using the same words as a language in which the behavioral rules are defined” (page 325, lines 5-8) as the experimental frame concept may be suitably utilized to couple with a given network model, generates input external events (cyber attack commands), monitor its running (consequences), and process its output (vulnerability).

With respect to claim 68, Sung teaches the limitation of “the modeling phase and the simulation phase are implemented by a user by means of a man/machine interface comprising a multi-view functionality, wherein a graphical representation of the system is presented to the user as several views” (page 331, lines 1-8) as a network security simulation system where users can set up initial conditions for simulation by using windows of each node. The can also try to test various cases by attaching attacker and analyzer to any particular node. Procedures of simulation can be checked by the packet-based animation and more detailed procedures can be checked through given windows.

With respect to claim 69, it is rejected in view of the same reasons as stated in the rejection of claim 68.

With respect to claim 71, it is noted that neither of Sung, Cohen, and Fox teach the limitation of "the behavioral rules for the components belonging to a view do not call by name upon components belonging to another view."

On the other hand, examiner takes the official notice that isolation of the elements is in the network system is not a novel concept and therefore, it would have been obvious to one of the ordinary skill in the art to provide no other ways for components to reference each other, other than through the information defined in the routing table controlled by the administrator to improve the security of the system.

With respect to claim 72, Sung teaches the views are associated with respective subsystems interconnected together via at least one common component (fig. 7).

With respect to claim 73, Sung fails to teach a higher view is associated with the information system as a whole, whereas one or more lower views are respectively associated with a determined subsystem of the information system. Fox teaches a multi-layered graphical display of the network whereby the administrator can drill down views into each component for more information about that component (col. 8, lines 45-55). Examiner supplies the same rationale as recited in the rejection of claim 45 for combining Sung and Fox.

As per claim 74, it rejected for the same reasons as recited in the rejection of claim 73.

As per claims 76 and 77, Sung fails to teaches the modeling phase further comprises a specification of one or more basic metrics associated respectively with the set of components wherein the basic metrics comprise at least one of a metric of effectiveness of parries [countermeasures]. Fox teaches the above limitations (col. 11, lines 22-27), as the node has risk assessment levels for determined the likelihood of being exploited. Risk assessment is another metric in determining how the system will cope with attacks. The claim is obvious because one of ordinary skill in the art can combine known methods which produce predictable results.

As per claim 78, Sung fails to teaches the simulation phase comprises a calculation of one more metrics of probability of mishap. Fox teaches this above limitation (col. 9, lines 27-32). Vulnerability assessment is another metric in determining how the system will cope with attacks. The claim is obvious because one of ordinary skill in the art can combine known methods which produce predictable results.

With respect to independent claim 83, it is rejected in view of the same reasons as stated in the rejection of independent claim 45.

With respect to claims 84 and 85, they are rejected in view of the reasons stated in the rejection of claim 68.

Claim 58 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sung, Cohen and Fox. as applied to claim 57 above, and further in view of Dowd et al. (US 7,315,801 B1).

With respect to claim 58, it is noted that neither of Sung, Cohen, or Fox teach the limitation of “the simulation phase furthermore comprises the building of a file or journal of the attacks, containing the log of the changes of the state of the components consequent upon successful attacks, in particular to allow subsequent processing by a user.”

On the other hand, Dowd teaches the abovementioned limitation (column 14, lines 11-13) as the security modeling system includes a log or a recorder which allows the system to play back the moves of an attacker or defender or both.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Dowd into the system of Sung, Cohen, and Fox because the system logs would provide the ability for the administrator to examine data retroactively.

Allowable Subject Matter

Claims 70 and 79-82 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and all intervening claims. The claim objections to all of the intervening claims as listed in the Office Action would have to be corrected as well.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431